*Report of the observer committee for e-voting process of IITKAA BoD elections 2010*

Prof. Rajat Moona

Department of CSE, IIT Kanpur

March 26, 2010

## Preamble

Mr. Abhay Bhushan, President, IIT Kanpur Alumni Association requested me to create one member observer committee with myself (with a possibility to involve additional alumni if necessary) and to report to the alumni on the erroneous mail sent by the system and other issues related to the e-voting and the fairness of the election process. This report explains such issues.

## The present e-voting system

The present e-voting system was developed for 2008 BoD elections and was used for the elections. The software was developed under my supervision by Akhilesh Srivastava who was the system administrator and web site manager in the Alumni Association Office at IIT Kanpur at that time. The software and its architecture were also independently evaluated and verified by Prof. Harish Karnick at IIT Kanpur.

The system operates in a fair manner and involves the anonymous voting using following architecture.

The system involves two independent officers who are together responsible for the conduct of election.

(a) Administrative Officer
(b) Election Officer

The job of the Administrative Officer is to facilitate the electronic voting while the vote is kept secret and anonymous jointly by the Election Officer and the Administrative Officer.

All voters are provided a “voterID” which is obtained using a secret key randomly generated in the beginning of the election process. The voterID created for a member can be used only once for the purposes of polling. The voterID is provided to the registered email addresses of the members by the Administrative Officer.

The e-voting system carries a “start” and “end” timestamps. The e-voting is permitted only during these time instants.

At the time of e-voting, the ballot is delivered through the web-link provided to the member. Along with this encryption software is also provided through the same web-link. The vote is encrypted on the machine of the voter twice. For this purpose, strong public-key encryption algorithms are used which are recognized as legal mechanisms under the IT-ACT 2000, subsequently modified in 2008 by the Govt. of India. Similar laws also exist in other countries as well.

The encryption is carried out with the public key of the Administrative Officer first. This is then counter-encrypted using the public key of the Election Officer. Two public keys are made available to the voter’s machine using the same encryption software. Only the resultant encrypted vote is made

available to the server by the voter's machine and is stored in the server database. The database stores the encrypted vote without any specific ID association with the vote. Thus the vote remains anonymous and its relation cannot be established with the voter. A separate database table keeps the flags of those voters who had cast their votes. It is important to note that the vote remains completely secure and anonymous in this process. Because of this strong feature it was adopted in 2008 elections and was found to work without any issues related to the privacy and integrity of the vote.

The corresponding private keys of the Administrative Officer and Election Officer are retained by them respectively and are used for decryption of encrypted votes for the counting purpose later.

The process of preparation of e-voting being used in the AA BoD Elections involves the following steps.

- Random key pairs are generated for Election Officer and Administrative Officer, and a random key is generated for the creation of voterIDs. Corresponding private keys are handed over to Election Officer and Administrative Officer.
- From AA database, the list of alumni is taken and all the members, whose email addresses are available, are sent a special voterID (as described above) that permits them to cast a vote.
- The rest of the election system is entirely independent of the AA access controls including the login and passwords as registered by the members. The election system subsequently depends only upon the voterID that had been generated.
- For online e-voting system, the system administrator is provided with certain web-based tools to generate voterIDs for members and mail it to them.
- The database is initialized to clear all flags to their default values.

## BoD Elections 2010

As per my understanding, based on flow of emails and the status of the database, the following are the sequence of events that took place for the BoD election 2010.

The call for nominations was sent by the Election Officer on January 18, 2010. The end of the nominations was set to February 7, 2010.

In the meanwhile, Mr. Navpreet Singh (Election Officer) met me along with Ms. Archana Jaiswal (Webmaster at Alumni Association) to understand the e-voting system. The same was explained by myself in person to both of them. Ms. Archana Jaiswal agreed to be the Administrative Officer and she was specifically asked to do the following tasks prior to start of the e-voting.

- Verify that the e-voting software is operational with the current set of the operating system and utilities. Since the same system was also used in 2008 elections for the first time, it was decided to verify the following – Generation of voterIDs, casting sample votes, preparation of results, checking the result etc. All such verifications were required to be done using dummy keys. The encryption-decryption process was also to be verified with the same set of dummy keys.
- Send the voterID to a small set of people who will then verify the mail contents, cast their votes and verify the correctness of the votes cast along with the webmaster.
- Subsequent to the successful verification, a new set of keys were to be generated for the BoD 2010 elections and the respective private keys to be stored with the Election Officer and the Administrative Officer.

The Election Officer was to keep in touch with the Administrative Officer to ensure that everything was in proper order. The system administrator reported to the Election Officer that everything was working as required. Election Officer then got in touch with me about this and consulted if the voterIDs could be generated. We analyzed the situation and agreed that the voterID could be generated. Prior to the generation of the voterIDs, the dummy keys were to be deleted and the database was to be initialized to prepare for the new election.

She was then asked to generate the voterIDs and mail them to all alumni members on 22nd February 2010.

## What went wrong

When the mail was received by the alumni, including the Election Officer, the content of the mail showed a list of candidates and voting dates which belonged to the last elections held in 2008. However the ballot had the correct list of candidates.

Mr. Navpreet Singh contacted me in the morning of 23rd February, informed about the wrong e-mail contents and asked for help to rectify the problem. He also told me that he had stopped the voting and sent an e-mail to members announcing the mistake and the nullification of all the votes that had been cast. Prof. Sameer Khandekar also called me to help in this process by putting about two days time.

As an alumnus, I had also received the email apology that was sent to all alumni, clarifying the situation and informing that the current voting process had been stopped and the e-voting would be re-launched only after resolving the issues.

## Investigations and Corrective Actions

Ms. Archana and Mr. Singh met me in the morning of the 23rd and we started looking at programs and databases for the possible source of errors. Prima-facie it appeared that the nomination slate that was sent through e-mail belonged to 2008 elections.

After about two hours of investigation, it was clear that Ms. Archana made an error in her verification and had not checked all the files containing programs and data. The investigations revealed that the old candidate list of 2008 elections was not modified in the email sending module. The email sending module is an ASP program that sends the e-mails containing voterID, list of candidates and the link and procedure to cast the vote. Since, the fact that the candidate list and other relevant details have to be changed in the email sending module was missed by the web master who generated the voterIDs, the wrong mails were generated and sent. When I asked for this explanation, she specifically told me that she expected the program to first generate the voterIDs and then send the mails subsequently possibly using another action from her.

At this point in time, we sat down and corrected this ASP program. Complete voting process was cross checked several times by starting a dummy voting process with dummy keys.

After all the elements were thoroughly checked and cross checked, the voting was started all over again on 26th February, 2010. For this, a new set of keys were generated. This step ensures those previously generated voterIDs, sent in the wrong mail, are rendered invalid and cannot be used in the new voting. The database was initialized, new dates for “start” and “end” of the e-voting were identified and put in the system.

The mails with new voterIDs and new slate of nominations were sent to all alumni, requesting them to cast their vote.

Subsequently while the election process and e-voting was on, some members raised suspicion on the process and the software. I have personally looked at each aspect of the software myself and find all such fears of tampering baseless. Some members also requested for changes in the closing dates and the Election Officer asked me if it is possible. While this could be possible, there was no simple way to do so. There were no user interfaces and one would be required to play with the databases directly. In the interest of the ongoing election process where a number of Alumni members had voted already, it was decided to not play around with such aspects and risk the existing database of the votes cast.

## Conclusions

I checked the databases and other programs and program generated outputs. Since I do not have the private keys of the Election Officer or of the Administrative Officer, I am not in the position to decrypt the secure vote. However from the contents of the database, things seem to be in order. It appears that the system has been working fine since the last restart of the e-voting.